Netskope.NSK300.v2026-01-25.q30

Exam Code:	NSK300
Exam Name:	Netskope Certified Cloud Security Architect
Certification Provider:	Netskope
Free Question Number:	30
Version:	v2026-01-25
# of views:	102
# of Questions views:	300
https://www.freecram.net/torrent/Netskope.NSK300.v2026-01-25.q30.html	

NEW QUESTION: 1
You are building an architecture plan to roll out Netskope for on-premises devices. You determine that tunnels are the best way to achieve this task due to a lack of support for explicit proxy in some instances and IPsec is the right type of tunnel to achieve the desired security and steering. What are three valid elements that you must consider when using IPsec tunnels in this scenario? (Choose three.)
A. Netskope Client behavior when on-premises
B. cipher support on tunnel-initiating devices
C. the categories to be blocked
D. bandwidth considerations
E. the impact of threat scanning performance
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Your Netskope Client tunnel has connected to Netskope; however, the user is not receiving any steering or client configuration updates What would cause this issue?
A. The client is unable to establish communication to add-on-[tenantl.goskope.com.
B. The client is unable to establish communication to gateway-(tenant|.goskope.com.
C. The Netskope Client service is not running.
D. An invalid steering exception was created in the tenant
Answer: (SHOW ANSWER)
When the Netskope Client service is not running, it cannot execute the necessary processes to receive steering or client configuration updates. The service must be active to establish communication with the Netskope cloud and apply the configurations and policies defined by the administrator.

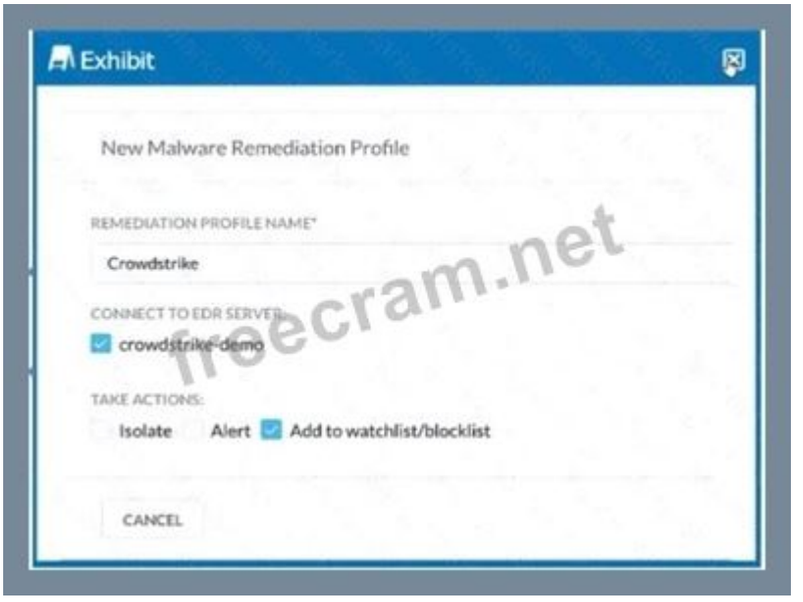
This information aligns with the Netskope Cloud Security Architect learning objectives and documents, which emphasize the importance of running client services for proper communication and functionality

NEW QUESTION: 3
You have multiple networking clients running on an endpoint and client connectivity is a concern. You are configuring co-existence with a VPN solution in this scenario, what is recommended to prevent potential routing issues?
A. Configure the VPN to split tunnel traffic by adding the Netskope IP and Google DNS ranges and set to Exclude in the VPN configuration.
B. Modify the VPN to operate in full tunnel mode at Layer 3. so that the Netskope agent will always see the traffic first.
C. Configure the VPN to full tunnel traffic and add an SSL Do Not Decrypt policy to the VPN configuration for all Netskope traffic.
D. Configure a Network Location with the VPN IP ranges and add it as a Steering Configuration exception.
Answer: (SHOW ANSWER)
* To prevent potential routing issues and ensure that the Netskope agent consistently sees the traffic first, it is recommended to modify the VPN to operate in full tunnel mode at Layer 3.
* In full tunnel mode, all traffic from the endpoint is routed through the VPN, including traffic destined for Netskope. This ensures that the Netskope agent can inspect and apply policies to all traffic, regardless of the destination.
* Layer 3 full tunnel mode provides better visibility and control over the traffic flow, reducing the risk of routing conflicts or bypassing the Netskope inspection. References:
* The answer is based on general knowledge of VPN configurations and their impact on traffic routing.

NEW QUESTION: 4
You are consuming Audit Reports as part of a Salesforce API integration. Someone has made a change to a Salesforce account record field that should not have been made and you are asked to venfy the previous value of the structured data field. You have the approximate date and time of the change, user information, and the new field value.
How would you accomplish this task?
A. Create a classic report and apply a query that filters on the changed field value.
B. Use the Application Events Data Collection within Advanced Analytics and filter on the changed field value.
C. Query Skope IT Page Events and look for the specific Page URL that was called under the Application section.
D. Query Skope IT for an Access Method of API Connector and search Application Event Details for the Old Value field using the User details and Edit Activity.
Answer: (SHOW ANSWER)

To verify the previous value of a structured data field in Salesforce after an unauthorized change, you would use Skope IT with an Access Method of API Connector. This method allows you to search the Application Event Details for the 'Old Value' field. By filtering with the user details and the edit activity, you can pinpoint the exact change and retrieve the original value of the field.
The approach is consistent with the Netskope Cloud Security Architect's guidelines for using API Data Protection with Salesforce. The documentation provides a detailed procedure for configuring Salesforce for API Data Protection, which includes the use of Netskope Audit Reports and the ability to track changes through the 'Old Value' field

NEW QUESTION: 5
Review the exhibit.



You are asked to integrate Netskope with Crowdstrike EDR. You added the Remediation profile shown in the exhibit.
Which action will this remediation profile take?
A. The malware will be quarantined.
B. The endpoint will be isolated.
C. The malware hash will be added as an IOC in Netskope.
D. The malware hash will be added as an IOC in Crowdstrike.
Answer: (SHOW ANSWER)

NEW QUESTION: 6
You are the network architect for a company using Netskope Private Access. Multiple users are reporting that they are unable to access an application using Netskope Private Access that was working previously. You have verified that the Real-time Protection policy allows access to the application, private applications are steered for the users, and the application is reachable from internal machines. You must verify that the application is reachable through Netskope Publisher
In this scenario, which two tools in the Netskope UI would you use to accomplish this task? (Choose two.)

A. Reachability Via Publisher in the App Definitions page
B. Troubleshooter tool in the App Definitions page
C. Applications in Skope IT
D. Clear Private App Auth under Users in Skope IT
Answer: (SHOW ANSWER)
In the scenario where users are unable to access an application through Netskope Private Access, and after verifying that the Real-time Protection policy allows access, the application is steered for the users, and it is reachable from internal machines, the next step is to verify the application's reachability through the Netskope Publisher. The two tools in the Netskope UI that would be used to accomplish this task are:
A). Reachability Via Publisher in the App Definitions page - This tool allows you to check if the application is reachable through the configured Publishers. It is essential to ensure that the application's connectivity is intact and that there are no issues with the Publishers themselves.
B). Troubleshooter tool in the App Definitions page - The Troubleshooter tool can help diagnose and resolve issues related to application reachability. It provides insights into potential problems and offers guidance on how to fix them.
These tools are designed to assist in troubleshooting and ensuring that applications are accessible through Netskope Private Access.
The explanation is based on the standard procedures for managing private applications and troubleshooting within the Netskope Private Access environment as outlined in the Netskope Knowledge Portal

NEW QUESTION: 7
Review the exhibit.

You installed Directory Importer and configured it to import specific groups ot users into your Netskope tenant as shown in the exhibit. One hour after a new user has been added to the domain, the user still has not been provisioned to Netskope.

What are three potential reasons for this failure? (Choose three.)

A. Directory Importer does not support ongoing user syncs; you must manually provision the user.

B. The server that the Directory Importer is installed on is unable to reach Netskope's add-on endpomt.

C. The user is not a member of the group specified as a filter

D. Active Directory integration is not enabled on your tenant.

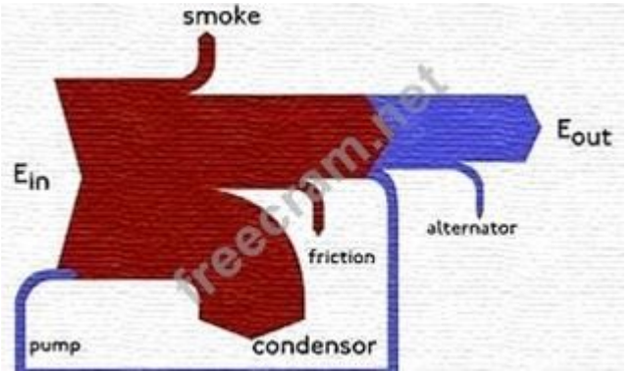
E. The default collection interval is 180 minutes, therefore a sync may not have run yet.

Answer: (SHOW ANSWER)

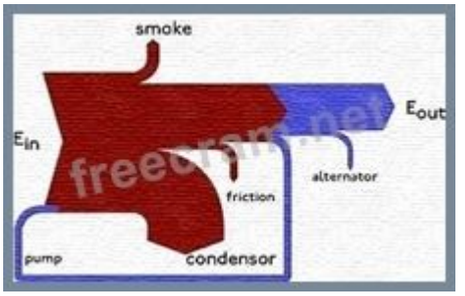
The three potential reasons for the failure of a new user not being provisioned to Netskope an hour after being added to the domain could be:

* B. The server that the Directory Importer is installed on is unable to reach Netskope's add-on endpoint:
If the server cannot connect to Netskope's endpoint, it cannot sync the user data. This could be due to network issues, incorrect configuration, or firewall restrictions1.
* C. The user is not a member of the group specified as a filter: The Directory Importer may be configured to import users from specific groups only. If the new user is not a member of these groups, they will not be imported into Netskope1.
* E. The default collection interval is 180 minutes, therefore a sync may not have run yet: The Directory Importer may be scheduled to sync every 180 minutes. If only an hour has passed, the sync process might not have occurred yet, and the user would not be provisioned until the next sync interval1.
These potential reasons are based on the standard operation and configuration of the Netskope Directory Importer as described in the Netskope Knowledge Portal and documentation

NEW QUESTION: 8
Your CISO asks that you to provide a report with a visual representation of the top 10 applications (by number of objects) and their risk score. As the administrator, you decide to use a Sankey visualization in Advanced Analytics to represent the data in an efficient manner.
In this scenario, which two field types are required to produce a Sankey Tile in your report? {Choose two.)
A. Dimension
B. Measure
C. Pivot Ranks
D. Period of Type
Answer: A,B (LEAVE A REPLY)



Sankey diagram



Sankey diagram

To produce a Sankey Tile in a report that visually represents the top 10 applications by number of objects and their risk score, you would need:
* Dimension (A): This field type would be used to represent the nodes in the Sankey visualization, which could be the applications in this case1.
* Measure (B): This field type would provide the weight of the links between the nodes, representing the number of objects or the risk score associated with each application1.
These two field types are essential for creating a Sankey visualization as they define the structure and flow of data between different stages or categories within the visualization.
The requirements for creating a Sankey visualization are based on the general principles of data visualization and the specific features of Sankey diagrams, which typically involve dimensions and measures to represent the flow of data1.

NEW QUESTION: 9
You configured a pair of IPsec funnels from the enterprise edge firewall to a Netskope data plane. These tunnels have been implemented to steer traffic for a set of defined HTTPS SaaS applications accessed from end-user devices that do not support the Netskope Client installation. You discover that all applications steered through this tunnel are non-functional.
According to Netskope. how would you solve this problem?
A. Restart the tunnel to stop the tunnel from flapping.
B. Downgrade from IKE v2 to IKE v1.
C. Install the Netskope root and intermediate certificates on the end-user devices.
D. Disable Perfect Forward Secrecy on the tunnel configuration.
Answer: (SHOW ANSWER)
When applications steered through an IPsec tunnel are non-functional, it is often due to the lack of proper trust establishment between the end-user devices and the Netskope data plane. The solution is to install the Netskope root and intermediate certificates on the end-user devices . This ensures that the devices recognize and trust the encrypted connection established by the IPsec tunnel, allowing the HTTPS SaaS applications to function correctly. Without these certificates, the devices may not be able to verify the security of the connection, leading to application failures. This solution is based on standard practices for securing IPsec tunnels and ensuring device compatibility with encrypted traffic steering, as outlined in Netskope's documentation on traffic steering and IPsec configuration

NEW QUESTION: 10
You want customers to configure Real-time Protection policies. In which order should the policies be placed in this scenario?

A. Threat, CASB, RBI, Web
B. RBI, CASB, Web, Threat
C. Threat, RBI, CASB, Web
D. CASB, RBI, Threat, Web
Answer: (SHOW ANSWER)

* When configuring Real-time Protection policies in Netskope, the recommended order is as follows:
* RBI (Risk-Based Index) Policies: These policies focus on risk assessment and prioritize actions based on risk scores. They help identify high-risk activities and users.
* CASB (Cloud Access Security Broker) Policies: These policies address cloud-specific security requirements, such as controlling access to cloud applications, enforcing data loss prevention (DLP) rules, and managing shadow IT.
* Web Policies: These policies deal with web traffic, including URL filtering, web categories, and threat prevention.
* Threat Policies: These policies focus on detecting and preventing threats, such as malware, phishing, and malicious URLs.
* Placing the policies in this order ensures that risk assessment and cloud-specific controls are applied before addressing web and threat-related issues. References:
* Netskope Security Cloud Introductory Online Technical Training
* Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training
* Netskope Certification Description
* Netskope Architectural Advantage Features

NEW QUESTION: 11
You are asked to ensure that a Web application your company uses is both reachable and decrypted by Netskope. This application is served using HTTPS on port 6443. Netskope is configured with a default Cloud Firewall configuration and the steering configuration is set for All Traffic.
Which statement is correct in this scenario?
A. Create a Firewall App in Netskope along with the corresponding Real-time Protection policy to allow the traffic.
B. Nothing is required since Netskope is steering all traffic.
C. Enable "Steer non-standard ports" in the steering configuration and add the domain and port as a new non-standard port
D. Enable "Steer non-standard ports" in the steering configuration and create a corresponding Real-time Protection policy to allow the traffic
Answer: (SHOW ANSWER)
To ensure that the web application using HTTPS on port 6443 is both reachable and decrypted by Netskope, the correct action is toenable "Steer non-standard ports" in the steering configuration and add the domain and port as a new non-standard port. This is because Netskope's default configuration steers standard HTTP
/HTTPS traffic, typically on ports 80 and 443.Since port 6443 is a non-standard port for HTTPS traffic, it requires explicit configuration to be steered through Netskope1.
The process for configuring non-standard ports in Netskope is detailed in the Netskope Knowledge Portal, which provides step-by-step instructions on how to steer HTTP(S) traffic over

non-standard ports1. This includes adding the specific non-standard port number in the steering configuration to ensure that traffic to and from that port is properly handled by Netskope.

NEW QUESTION: 12
A hospital has a patient form that they share with their patients over Gmail. The blank form can be freely shared among anyone. However, if the form has any information filled out. the document is considered confidential.
Which rule type should be used in the DLP profile to match such a document?
A. Use fingerprint classification.
B. Use a dictionary rule for all your patient names.
C. Use Exact Match with patient names
D. Use predefined DLP Rule(s) that match the patient name.
Answer: (SHOW ANSWER)
The appropriate rule type to use in the DLP profile for a document that is considered confidential when filled out isfingerprint classification. Fingerprinting is a method used to identify and protect sensitive data within documents. It works by creating a digital fingerprint of a file, which can then be used to detect any copies or derivatives of that file.In this case, fingerprinting would allow the hospital to differentiate between the blank patient form, which can be freely shared, and the same form with patient information filled out, which is confidential1.
Netskope's DLP rules can contain elements such as predefined data identifiers, custom data identifiers, keyword identifiers from a dictionary file, RegEx expressions, and exact match criteria1.For this specific use case, fingerprint classification is the most effective method as it can accurately detect the presence of filled- out information in the forms, which is crucial for maintaining patient confidentiality as per HIPAA regulations1.

NEW QUESTION: 13
Your client is an NG-SWG customer. They are going to use the Explicit Proxy over Tunnel (EPoT) steering method. They have a specific list of domains that they do not want to steer to the Netskope Cloud.
What would accomplish this task"
A. Define exception domains in the PAC file.
B. Define exceptions in the Netskope steering configuration
C. Create a real-time policy with a bypass action.
D. Use an SSL decryption policy.
Answer: A (LEAVE A REPLY)
To accomplish the task of not steering specific domains to the Netskope Cloud while using the Explicit Proxy over Tunnel (EPoT) steering method, you wouldddefine exception domains in the PAC file (A).This is because the PAC file is used to specify which domains should bypass the proxy and connect directly, thus allowing for granular control over the traffic that is steered to Netskope1.

The use of PAC files for steering exceptions is a standard practice in proxy configurations and is supported by Netskope's EPoT steering method as outlined in their documentation1.

NEW QUESTION: 14
You are architecting a Netskope steering configuration for devices that are not owned by the organization The users could be either on-premises or off-premises and the architecture requires that traffic destined to the company's instance of Microsoft 365 be steered to Netskope for inspection.
How would you achieve this scenario from a steering perspective?
A. Use DPoP and Secure Forwarder
B. Use reverse proxy.
C. Use IPsec and GRE tunnels.
D. Use explicit proxy and the Netskope Client
Answer: (SHOW ANSWER)

NEW QUESTION: 15
Review the exhibit.

You are the proxy administrator for a medical devices company. You recently changed a pilot group of users from cloud app steering to all Web traffic. Pilot group users have started to report that they receive the error shown in the exhibit when attempting to access the company intranet site that is publicly available. During troubleshooting, you realize that this site uses your company's internal certificate authority for SSL certificates.
Which three statements describe ways to solve this issue? (Choose three.)
A. Import the root certificate for your internal certificate authority into Netskope.
B. Bypass SSL inspection for the affected site(s).
C. Create a Real-time Protection policy to allow access.
D. Change the SSL Error Settings from Block to Bypass in the Netskope tenant.
E. Instruct the user to proceed past the error message
Answer: (SHOW ANSWER)
* A. Import the root certificate for your internal certificate authority into Netskope:
* This step ensures that Netskope recognizes and trusts SSL certificates issued by your company's internal certificate authority. By importing the root certificate, you enable proper SSL inspection and validation for internal sites.
* B. Bypass SSL inspection for the affected site(s):

* Since the intranet site uses your company's internal certificate authority, bypassing SSL inspection for this specific site allows users to access it without encountering SSL errors.
* D. Change the SSL Error Settings from Block to Bypass in the Netskope tenant:
* Adjusting the SSL Error Settings to "Bypass" allows users to proceed past SSL errors, including self-signed certificate errors. This ensures uninterrupted access to the intranet site. References:
* Netskope Security Cloud Introductory Online Technical Training
* Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training
* Netskope Cloud Security Certification Program

NEW QUESTION: 16
Given the following:

```
user eq 'user@company.com' and access_method eq 'Client' and activity eq 'Download' or activity eq 'Upload' and site eq 'Amazon S3'
```

Which result does this Skope IT query provide?
A. The query returns all events of user@company.com downloading or uploading to or from the site
'Amazon S3" using the Netskope Client.
B. The query returns all events of an IP address downloading or uploading to or from Amazon S3 using the Netskope Client.
C. The query returns all events of everyone except user@company.com downloading or uploading to or from the site "Amazon S3" using the Netskope Client.
D. The query returns all events of user@company.com downloading or uploading to or from the application "Amazon S3" using the Netskope Client.
Answer: (SHOW ANSWER)
* The given Skope IT query specifies the following conditions:
* User equals 'user@company.com'
* Access method equals 'Client'
* Activity equals 'Download' or 'Upload'
* Site equals 'Amazon S3'
* The query combines these conditions using logical operators (AND and OR).
* The result of this query will include all events where the specified user ('user@company.com') is either downloading or uploading data to or from the site 'Amazon S3' using the Netskope Client.
* It does not include events related to other users or IP addresses. References:
* Netskope Security Cloud Introductory Online Technical Training
* Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training

NEW QUESTION: 17
You are troubleshooting an issue with users who are unable to reach a financial SaaS application when their traffic passes through Netskope. You determine that this is because of IP restrictions in place with the SaaS vendor. You are unable to add Netskope's IP ranges at this time, but need to allow the traffic.
How would you allow this traffic?
A. Use NPAto implement Source IP anchonng so the traffic will egress from the corporate data center.
B. Use Explicit Proxy Over Tunnel (EPoT) so the traffic will egress from the corporate data center.
C. Use Cloud Explicit Proxy so the traffic will egress from the corporate data center
D. Use an IPsec tunnel to forward traffic so it will egress from the corporate data center
Answer: (SHOW ANSWER)
To allow traffic to a financial SaaS application that is being blocked due to IP restrictions, the best option is to useCloud Explicit Proxy. This method allows traffic to egress from the corporate data center without requiring Netskope's IP ranges to be added to the SaaS vendor's allowlist.By configuring an allowlist in the Cloud Explicit Proxy settings, you can add any source egress IP addresses for your on-premises users, and Netskope will allow the traffic from the added user and IP address without authenticating1.
The process for configuring an allowlist in Cloud Explicit Proxy to manage unauthenticated traffic from specific IP addresses is detailed in the Netskope Knowledge Portal1. This solution is suitable for scenarios where adding Netskope's IP ranges to the SaaS vendor's IP restrictions is not feasible.

NEW QUESTION: 18
Your company just had a new Netskope tenant provisioned and you are asked to create a secure tenant configuration. In this scenario, which two default settings should you change? {Choose two.)
A. Change Safe Search to Disabled
B. Change Untrusted Root Certificate to Block.
C. Change the No SNI setting to Block.
D. Change "Disallow concurrent logins by an Admin" to Enabled.
Answer: (SHOW ANSWER)
For a new Netskope tenant provisioned, to create a secure tenant configuration, you should consider changing the following default settings:
* B. Change Untrusted Root Certificate to Block: This setting will ensure that any traffic coming from an untrusted root certificate is blocked, which is a critical security measure to prevent man-in-the-middle attacks and other types of cyber threats1.

* D. Change "Disallow concurrent logins by an Admin" to Enabled: This setting will prevent multiple concurrent logins by the same admin account, which is an important security control to mitigate the risk of unauthorized access.If an admin's credentials are compromised, this setting will help limit the potential damage by ensuring that only one session can be active at a time1.
These changes are part of the recommended security hardening guidelines for Netskope tenants to enhance the overall security posture of the tenant environment.
The recommendations for changing default settings for a secure tenant configuration are based on Netskope' s security hardening guidelines, which provide detailed instructions on how to enhance the security of Netskope products and components deployed in customer environments1.

NEW QUESTION: 19
You are using Netskope CSPM for security and compliance audits across your multi-cloud environments. To decrease the load on the security operations team, you are researching how to auto-re mediate some of the security violations found in low-risk environments.
Which statement is correct in this scenario?
A. Netskope does not support automatic remediation of security violation results due to the high risk associated with it.
B. You can use Netskope API-enabled Protection for auto-remediation of security violation results.
C. You can use Netskope Auto-remediation frameworks from the public Netskope GitHub Open Source repository for auto-re mediation of security violation results.
D. You can use Netskope Cloud Exchange for auto-remediation of security violation results.
Answer: (SHOW ANSWER)
Netskope supports automatic remediation of security violations through its Auto-Remediation frameworks, which are available in the public Netskope GitHub Open Source repository. These frameworks allow for the automatic mitigation of risks associated with security misconfigurations in your cloud environment. The Netskope Auto-Remediation framework for AWS, for example, deploys a set of AWS Lambda functions that query the Netskope API at scheduled intervals and automatically mitigates supported violations1. Similarly, there are frameworks for GCP and other cloud environments that follow the same principle2. This capability is particularly useful for low-risk environments where the security operations team's workload can be reduced by automating the remediation process.
The answer is based on the information provided by Netskope's community resources and documentation, which detail the use of their Auto-Remediation frameworks for various cloud platforms

NEW QUESTION: 20

You deployed Netskope Cloud Security Posture Management (CSPM) using pre-defined benchmark rules to monitor your cloud posture in AWS, Azure, and GCP. You are asked to assess if you can extend the Netskope CSPM solution by creating custom rules for each environment.
Which statement is correct?

A. Custom rules using Domain Specific Language are only available when using SSPM.
B. You will need to evaluate SaaS Security Posture Management (SSPM) in addition to CSPM so that rules applied to GCP will align with Google Workspace
C. With Netskope CSPM, you can create custom rules using Domain Specific Language for AWS. Azure, but not for GCP.
D. With Netskope CSPM, you can create custom rules using Domain Specific Language for AWS. Azure, and GCP
Answer: (SHOW ANSWER)
Netskope Cloud Security Posture Management (CSPM) allows for the creation of custom rules using Domain Specific Language (DSL) for all three major cloud platforms: AWS, Azure, and GCP. This capability is integral to CSPM and enables organizations to tailor their security posture assessments to their specific needs across different cloud environments.
The ability to create custom rules using DSL within Netskope CSPM for AWS, Azure, and GCP is documented in the Netskope Knowledge Portal. It provides detailed instructions on how to build custom rules under Policies > Security Posture > Profiles & Rules for security assessment of resources across these cloud platforms

NEW QUESTION: 21
You want to verify that Google Drive is being tunneled to Netskope by looking in the nsdebuglog file. You are using Chrome and the Netskope Client to steer traffic. In this scenario, what would you expect to see in the log file?
A.

```
2022/01/0 01:00:00.001010 stAgentNE p752b t28da7 info tunnel.cpp:712 nsTunnel TLS [sessId 502] Tunneling flow from addr:
1.0.0.1:64000, process: google drive to host: play.googleapis.com, addr: 172.217.4.46:443 to nsProxy
```

B.

```
2022/01/0 01:00:00.001010 stAgentNE p752b t28da7 info tunnel.cpp:712 nsTunnel TLS [sessId 502] Tunneling flow from addr:
1.0.0.1:63720, process: google chrome helper to host: drive.google.com, addr: 172.217.4.46:443 to nsProxy
```

C.

```
2022/01/0 01:00:00.001010 stAgentNE p752b t28da7 info bypassAppMgr.cpp:538 BypassAppMgr Bypassing UDP flow to process
google chrome helper ip: 172.217.4.46, Port: 443, host: drive.google.com
```

D.

```
2022/01/0 01:00:00.001010 stAgentNE p752b t28da7 info AppProxyProvider.mm:303 main New UDP flow: Process = google chrome
helper, IP:Port = [8.8.8.8:53]
```

Answer: (SHOW ANSWER)
When verifying that Google Drive traffic is being tunneled to Netskope using Chrome and the Netskope Client, you would expect to see log entries indicating that the traffic is being directed through Netskope's proxy. Specifically, Option A is correct as it shows the process "google drive" being tunneled tonsProxy. The log entry for Option A indicates that a TLS tunneling flow from a local address and process (Google Drive) is being directed to a host (play.googleapis.com) and

then to Netskope's proxy (nsProxy).This is consistent with how Netskope tunnels specified traffic for security and policy enforcement1.
The expected log entries are based on the standard operation of Netskope Client and how it steers traffic to Netskope's cloud services, as detailed in Netskope's documentation1.

NEW QUESTION: 22
Your company purchased Netskope's Next Gen Secure Web Gateway You are working with your network administrator to create GRE tunnels to send traffic to Netskope Your network administrator has set up the tunnel, keepalives. and a policy-based route on your corporate router to send all HTTP and HTTPS traffic to Netskope. You want to validate that the tunnel is configured correctly and that traffic is flowing.
In this scenario, which two statements are correct? (Choose two.)
A. You can use your local router or network device to verify that keepalives are being received and traffic is flowing to Netskope.
B. You must use your own monitoring tools to verify that the tunnel is up.
C. You can verify that the tunnel is up and receiving traffic in the Netskope UI under Settings > Security Cloud Platform > GRE.
D. You can verify that the tunnel is up in the Netskope Trust portal at https://trust netskope.com/.
Answer: (SHOW ANSWER)
To validate that the GRE tunnel is configured correctly and that traffic is flowing to Netskope, the correct statements are:
* A: You can use your local router or network device to verify that keepalives are being received and traffic is flowing to Netskope. This is a standard method for checking the health and activity of a GRE tunnel.
* C: You can verify that the tunnel is up and receiving traffic in the Netskope UI under Settings > Security Cloud Platform > GRE. This is a feature provided by Netskope to monitor the status of GRE tunnels directly from the Netskope interface12.
Statement B is incorrect because Netskope provides its own tools for monitoring the status of the tunnel. Statement D is incorrect because the Netskope Trust portal provides information on the overall service status and updates, not specific tunnel status3.
The references for these answers can be found in the Netskope Knowledge Portal, which provides detailed guidance on configuring and validating GRE tunnels12. Additionally, the Netskope Community Forum offers insights and solutions for deploying and monitoring GRE tunnels

NEW QUESTION: 23
You are implementing a solution to deploy Netskope for machine traffic in an AWS account across multiple VPCs. You want to deploy the least amount of tunnels while providing connectivity for all VPCs.
How would you accomplish this task?
A. Use IPsec tunnels from the AWS Virtual Private Gateway.

B. Use GRE tunnels from the AWS Transit Gateway.
C. Use GRE tunnels from the AWS Virtual Private Gateway
D. Use IPsec tunnels from the AWS Transit Gateway.
Answer: D (LEAVE A REPLY)
The best approach to deploy Netskope for machine traffic across multiple VPCs in an AWS account with the least amount of tunnels while providing connectivity for all VPCs is to useIPsec tunnels from the AWS Transit Gateway.This method allows you to use the same Site-to-Site VPN connection to Netskope for multiple VPCs, thus minimizing the number of tunnels required12. The AWS Transit Gateway acts as a network transit hub, enabling you to connect your VPCs and on-premises networks through a central point of management and control.Using IPsec tunnels with the AWS Transit Gateway ensures that all VPCs connected to it utilize the same IPsec tunnel between the transit gateway and Netskope POP1.
Detailed guidance on configuring IPsec VPN tunnels between your AWS Transit Gateway and Netskope POPs can be found in the Netskope Knowledge Portal1.Additionally, the Netskope Community Forum provides insights on setting up IPsec Tunnels for AWS egress traffic, which includes information relevant to deploying Netskope across multiple VPCs2.

NEW QUESTION: 24
You need to extract events and alerts from the Netskope Security Cloud platform and push it to a SIEM solution. What are two supported methods to accomplish this task? (Choose two.)
A. Use Cloud Ticket Orchestrator.
B. Use Cloud Log Shipper.
C. Stream directly to syslog.
D. Use the REST API.
Answer: (SHOW ANSWER)
To extract events and alerts from the Netskope Security Cloud platform and integrate them with a SIEM (Security Information and Event Management) solution, you can utilize the following supported methods:
* Cloud Log Shipper (CLS):
* The Cloud Log Shipper is designed to forward Netskope logs to external systems, including SIEMs.
* It allows you to export logs in real-time or batch mode to a destination of your choice.
* By configuring CLS, you can ensure that Netskope events and alerts are sent to your SIEM for further analysis and correlation.
Reference: Netskope Documentation on Cloud Log Shipper
REST API:
The Netskope Security Cloud provides a comprehensive REST API that allows you to programmatically retrieve data, including events and alerts.
You can use the REST API to query specific logs, incidents, or other relevant information from Netskope.
By integrating with the REST API, you can extract data and push it to your SIEM solution.

Reference: Netskope REST API Documentation
References:
Netskope Cloud Security
Netskope Resources
Netskope Documentation
These methods ensure seamless data flow between Netskope and your SIEM, enabling effective security monitoring and incident response.

NEW QUESTION: 25
Users in your network are attempting to reach a website that has a self-signed certificate using a GRE tunnel to Netskope. They are currently being blocked by Netskope with an SSL error. How would you allow this traffic?
A. Configure a Do Not Decrypt SSL Decryption rule to allow traffic to pass.
B. Configure a Real-time Protection policy with the action set to Allow.
C. Set the No SNI setting in Netskope to Bypass.
D. Ensure that the users add the self-signed certificate to their local certificate store.
Answer: (SHOW ANSWER)
To allow traffic from a website with a self-signed certificate that is being blocked by Netskope with an SSL error, the correct action is to configure aDo Not Decrypt SSL Decryption rule. This rule will allow the traffic to pass without being decrypted, thus bypassing the SSL error caused by the self-signed certificate.This is a common practice for handling traffic from trusted internal applications or specific external sites that use self- signed certificates1.
The Netskope Community Forum discusses the application of exceptions for sites with self-signed certificates and the use of SSL decryption policies to bypass the blocking1.Additionally, the Netskope Knowledge Portal provides information on managing error settings and configuring SSL decryption rules2.

NEW QUESTION: 26
A company wants to capture and maintain sensitive PII data in a relational database to help their customers.
There are many employees and contractors that need access to sensitive customer data to perform their duties The company wants to prevent the exfiltration of sensitive customer data by their employees and contractors.
In this scenario. what would satisfy this requirement?
A. regular expression
B. exact data match
C. fingerprinting
D. machine learning
Answer: (SHOW ANSWER)

NEW QUESTION: 27

You have enabled CASB traffic steering using the Netskope Client, but have not yet enabled a Real-time Protection policy. What is the default behavior of the traffic in this scenario?

A. Traffic will be blocked and logged.

B. Traffic will be allowed and logged.

C. Traffic will be blocked, but not logged.

D. Traffic will be allowed, but not logged.

Answer: (SHOW ANSWER)

In the scenario where CASB traffic steering is enabled using the Netskope Client without a Real-time Protection policy being activated, the default behavior of the traffic is toallow and log it (B). This means that the traffic will not be blocked; instead, it will be permitted to pass through and will be recorded for monitoring and analysis purposes.This default setting ensures visibility into the traffic and user activities without immediately enforcing a block, allowing for a period of observation and policy tuning before potentially more restrictive actions are taken1.

The default behavior of traffic steering in Netskope, including the logging of allowed traffic, is detailed in Netskope's best practices and community discussions on Real-time Protection policies1.

NEW QUESTION: 28

A recent report states that users are using non-sanctioned Cloud Storage platforms to share data Your CISO asks you for a list of aggregated users, applications, and instance IDs to increase security posture Which Netskope tool would be used to obtain this data?

A. Advanced Analytics

B. Behavior Analytics

C. Applications in Skope IT

D. Cloud Confidence Index (CCI)

Answer: (SHOW ANSWER)

To obtain a list of aggregated users, applications, and instance IDs, especially when dealing with non- sanctioned Cloud Storage platforms, the Advanced Analytics (A) tool within Netskope would be used.

Advanced Analytics provides in-depth visibility into cloud app usage and activities. It allows security teams to create detailed reports and dashboards that can help identify risks and ensure compliance with company policies by analyzing user behavior, application access, and data movement across the organization1.

The capabilities of the Advanced Analytics tool are outlined in Netskope's documentation and resources, which describe its use for gaining insights into cloud application usage and security posture

NEW QUESTION: 29

You deployed the Netskope Client for Web steering in a large enterprise with dynamic steering. The steering configuration includes a bypass rule for an application that is IP restricted. What is the source IP for traffic to this application when the user is on-premises at the enterprise?

A. Loopback IPv4
B. Netskope data plane gateway IPv4
C. Enterprise Egress IPv4
D. DHCP assigned RFC1918 IPv4
Answer: (SHOW ANSWER)
* When a user is on-premises at the enterprise and accesses an application that is IP restricted, the source IP for traffic to this application is the Enterprise Egress IPv4 address.
* The Enterprise Egress IP represents the external IP address of the enterprise network as seen by external services or applications.
* This IP address is used for communication between the user's device and external resources, including applications that are IP restricted. References:
* The answer is based on general knowledge of networking concepts and how IP addresses are used in enterprise environments.

NEW QUESTION: 30
Your organization's software deployment team did the initial install of the Netskope Client with SCCM. As the Netskope administrator, you will be responsible for all up-to-date upgrades of the client. Which two actions would be required to accomplish this task9 (Choose two.)

A. In the Client Configuration, set Upgrade Client Automatically to Latest Release.
B. Set the installmode-IDP flag during the original Install.
C. Set the autoupdate-on flag during the original Install.
D. In the Client Configuration, set Upgrade Client Automatically to Specific Golden Release.
Answer: (SHOW ANSWER)
To ensure that the Netskope Client is always up-to-date with the latest upgrades, two actions are required.
First, in the Client Configuration, the administrator should set the option to Upgrade Client Automatically to Latest Release. This setting ensures that the client will automatically update to the most recent version available. Second, during the original installation of the Netskope Client, the autoupdate-on flag should be set.
This flag enables the auto-update feature, allowing the client to receive and apply updates as they are released.
The information is based on the Netskope Client deployment options and upgrade process as detailed in the Netskope Knowledge Portal